The ISC Int'l Journal of Information Security
ISeCure

January 2009, Volume 1, Number 1 (pp. 1–2)
http://www.isecure-journal.org

On Behalf of the Editorial Board

Editorial

It is with great pleasure to bring you the first issue of ISeCure, the ISC's international journal on information security. Founded in 1999, ISC (Iranian Society of Cryptology) is a scientific, non-governmental, and non-profit organization whose main mission includes expansion of knowledge boundaries and publishing information security research results. While there are many world-wide refereed journals in the areas of Electrical Engineering, Communication Engineering, Computer Science & Engineering, and Applied Mathematics, there are a few journals focused on information security. Accordingly, following five successful conferences on Information Security and Cryptology, ISC decided to publish ISeCure, dedicated to research in information security and cryptology.

ISeCure aims to provide a forum for the publication of high-quality original research results in areas of information security and cryptology- from theoretical to applied issues. The topics include theoretical foundations of cryptology, formal methods in information security, information hiding, cryptographic hardware & embedded systems, and applications of security in various fundamental components of information technology-Computer Networks, Operating Systems, Databases, Software Systems, and E-business.

The editorial process in ISeCure assures the selection of high-quality manuscripts. It includes an initial inspection of the manuscript organization and content in the prescreening phase, assignment of a paper editor and several international referees, and final decision by the Editorial Board. For more details about all aspects of the journal, including review process, scope, and author's guide, please refer to the journal website (www.isecure-journal.org). The website also includes the electronic version of the papers published in ISeCure free of charge.

For the first issue, 23 manuscripts have been considered, of which only five have found their way into publication. The first paper proposes a steganalysis approach to the MPVD steganography method. The proposed approach employs a multi-layer neural network, structured based on the statistical alterations that occur in the embedded image, which yields the overall steganalysis result through a voting procedure. Using the proposed method, it is claimed that the existence of a secret message in the MPVD-based steganography can be revealed accurately at some embedding rates.

The second paper proposes a mutual entity authentication using the TESLA protocol. The proposed solution achieves a secure bilateral authentication mechanism with considerable decrease in the cost of the call setup time and the required connection bandwidth. The proposed authentication protocol is compatible with the GSM standard and utilizes GSM's capability maximally.

The third paper describes an attack on the Fuzzy Vault scheme. It is assumed that the attacker has access to multiple vaults locked by the same key and uses a non-maximal vault size. The attack effectively reduces the vault size by identifying and removing chaff points. As the vault size decreases, the rate at which chaff points are identified increases exponentially. The paper also discusses several possible defenses against the attack.

The forth paper proposes a context-aware mandatory access control model, called CAMAC, which not only preserves the confidentiality and integrity of information as specified in the traditional mandatory access control models, but also handles dynamic adaptation of access control policies to the context, and context-sensitive class association. The model is capable of being deployed in multilevel security environments and where the

ISSN: 2008-2045

information flow control with context-sensitive security classes is necessary. Furthermore, the proposed model can express various mandatory access control policies.

The fifth paper takes advantage of the notion of transition systems to specify authentication for parallel multiple session execution. The parallel composition of the protocol parties and the enemy is considered-which should be initiator-fail and responder-fail free. To express the notion of authentication, agents' scope and agents' recognizability are considered. These notions are formalized through a process algebra equipped with cryptographic primitives, which can be translated to μCRL. Finally, it is shown that verification of t-security of a protocol (i.e. initiator-fail and responder-fail free for t completion runs) is decidable.

A new journal can only be successful as the result of collaborative efforts of a large number of commited individuals. Remarkable among these are the members of the editorial board, the paper editors, the members of the advisory board, and the dedicated staff of ISeCure. Many of the reviewers have made a praiseworthy effort to assist the authors in improving their manuscripts. We would like to express our sincere appreciation to all of them. We would also like to acknowledge the authors who have submitted their manuscripts to the journal, for they have provided the inspiration for the efforts of all the rest of us. We would also take this opportunity to solicit more submissions; we hope that this first issue will encourage potential authors. Any comments or suggestions are welcome.

Mohammad Reza Aref

President, Iranian Society of Cryptology (ISC)

Rasool Jalili

Editor-in-Chief, ISeCure

Mohammad Reza Aref was born in Iran in 1951. He received his B.Sc. in 1975 from the University of Tehran, his M.Sc. in 1976 and his Ph.D. in 1980 from Stanford University, Stanford, California, all in Electrical Engineering. From 1994 to 1997 he was the Chancellor of the University of Tehran, and from 1997 to 2000 he served as the Minister of Information and Communications Technology (ICT) of Iran. From 2000 to 2005, he was the Vice President of the Islamic Republic of Iran. He was a faculty member of Isfahan University of Technology from 1982 to 1995; He has been a Professor of Electrical Engineering at Sharif University of Technology since 1995. He has published more than 180 papers in Communications and Information Theory and Cryptography in international journals and conference proceedings. He is currently the president of ISC (Iranian Society of Cryptology).

Rasool Jalili was born in Iran in 1961. He received his bachelor's degree in Computer Science from Ferdowsi University of Mashhad in 1985, and his master's degree in Computer Engineering from Sharif University of Technology in 1989. He received his Ph.D. in Computer Science from The University of Sydney, Australia, in 1995. He then joined the Department of Computer Engineering, Sharif University of Technology, Tehran, Iran, in 1995. He has published more than 130 papers in Computer Security and Pervasive Computing in international journals and conferences proceedings. He is now an associate professor. His research interests include such areas as access control, vulnerability analysis, and database security—which he conducts at his network security laboratory (NSC, nsc.sharif.edu).